Local cybersecurity pressures on the rise

The cybersecurity sector in South Africa continues to grow at pace – with a compound annual growth rate (CAGR) of 12,97 percent between 2023 to 2028 predicted by Mordor Intelligence.

And this comes as no real surprise. Global attacks have increased, rising by seven percent per week in Q1 2023 compared to the same quarter in 2022, according to Check Point Software Technologies, with each organisation facing an average of 1,248 attacks per week. African businesses are under even greater threat, the cybersecurity company said, at an average of 1,983 attacks on a weekly basis. In addition, over the same period, one in 15 African organisations were targeted in ransomware attacks.

“Looking at the continent, South Africa in particular has been under siege, rated at sixth worldwide for cybercrime density according to the local Council for Scientific and Industrial Research (CSIR), which estimates that the impact of cybercrime on the South African economy is at around R2.2 billion per annum,” explains Brian Smith, Business Unit Manager at Datacentrix, a leading hybrid ICT systems integrator and managed services provider.

“Looking at the continent, South Africa in particular has been under siege, rated at sixth worldwide for cybercrime density according to the local Council for Scientific and Industrial Research (CSIR), which estimates that the impact of cybercrime on the South African economy is at around R2.2 billion per annum.

More attacks, fewer experts

He continues: “In South Africa we're dealing with what is essentially a double whammy: a swiftly multiplying number of cyberattacks and a dearth of local cybersecurity skills. Demand for cybersecurity skills is at an all-time high – and growing – but we're facing complex challenges in South African within this space.”

As per Fortinet’s 2023 Cybersecurity Skills Gap report, staffing up to strengthen security is a top board priority for organisations worldwide. Most boards recommend hiring IT and cybersecurity staff, states the report, with 83 percent of leaders indicating that their board recommended increasing IT and cybersecurity headcount in 2022, up from 76 percent in 2021, and 85 percent of boards that govern organisations with more than 5,000 employees recommended increasing IT security headcount.

“It's clear that the need for good cybersecurity skills is there. However, factors like emigration and 'semi-gration', where workers remain in South Africa but their skills are being leveraged outside the country, have played a role in widening the current skills breach locally,” says Smith.

Another issue is the vast array of cybersecurity products available on the market today, he adds. “While twenty years ago, there may have been around 5,000 solutions available, today we're looking at closer to 500,000. How do you choose which ones are the most important? And how does your cybersecurity team stay on top of the many required certifications and skills level requirements?”

> The SECaaS approach is growing in popularity, as it offers organisations a number of benefits, including the ability to scale this service as it is required. This is an attractive option, as companies can then avoid potentially overspending on security services that may not benefit them.

Brian Smith, Business Unit Manager at Datacentrix

Could Security as a Service be the answer?
According to Smith, a good rule of thumb would be to look at recent analyst firms' reports and identify what they're touting as the top five or six cybersecurity vendors.

Businesses could also look at how artificial intelligence (AI) can assist in automating and eliminating some of the more manual tasks, like data scanning, and the good news here is that we are seeing signs of AI-readiness within several cybersecurity products.

Another option – and one that would remove skills and certification worries from the business – would be to go the Security as a Service (SECaaS) route. Here, an organisation would opt for an outsourced, cloud-based cybersecurity offering that could include threat detection, data protection, email, network and database security, intrusion management, identity and access management, data loss prevention, and more.

“The SECaaS approach is growing in popularity, as it offers organisations a number of benefits, including the ability to scale this service as it is required. This is an attractive option, as companies can then avoid potentially overspending on security services that may not benefit them.

“Aside from the cost saving aspect, SECaaS also provides access to the most recent tools and updates, as well as to skilled cybersecurity experts, thereby freeing up an internal ICT team instead of adding more pressure.”

As a potential SECaaS partner, Datacentrix offers an end-to-end security service, including its state-of-the-art Security Operations Centre (SOC), manned by a team that is more than 50 strong.

Datacentrix has built a cybersecurity ecostructure that incorporates solutions from leading cybersecurity vendors such as BeyondTrust, Check Point, Forescout, CLoudflare, F5, GYTPOL, Fortinet, IBM, OKTA, Mimecast, Palo Alto Networks, Tenable, Trend Micro, ransomware protection backups with Rubrik and more. Not only do we maintain the highest levels of partnership status and certification levels with these partners, we've also ensured that they are integrated together within our SOC.

Says Smith: “The security landscape is changing on a daily basis, making it increasingly difficult for internal cybersecurity teams to effectively protect against threats. This also has a direct effect on the Chief Information Security Officer (CISO), as you can no longer plan a cybersecurity strategy for the next 24 to 36 months.

“With the right SECaaS partner behind them, businesses can review plans more regularly – at least every six months – creating shorter-term plans together and ensuring that the right skills and solutions are in place to achieve these goals.”

For more information on Datacentrix’s Security Services offering, please visit www.datacentrix.co.za/security-services.html